

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

V.

ANDREW KASNETZ,

Defendant.

CASE NO. 3:18-cr-00345

(HEARING REQUESTED)

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Defendant, Andrew Kasnetz, through undersigned counsel, submits this Motion to Suppress Evidence and Request for Evidentiary Hearing (the “Motion”). Pursuant to Fed.R.Crim.P. 12(b), Defendant Kasnetz respectfully moves this Court to suppress any and all evidence seized as a result of an unreasonable search used to use obtain a search warrant, and the further unreasonable search and seizure of items in his home on February 20, 2018, conducted in violation of the Fourth Amendment of the United States Constitution.

I. PROCEDURAL BACKGROUND

1. Defendant Kasnetz has been indicted on the following charges: receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2) (Count 1); and possession of prepubescent child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) (Count 2 & 3). Mr. Kasnetz has pled not guilty to these charges.

2. Trial is set for August 23, 2021.

II. PREHEARING STATEMENT OF FACTS¹

¹ This recitation of facts is gleaned from the Indictment. This recitation is not intended as a stipulation of facts.

3. The Indictment alleges that on or about February 20, 2018, using a peer-to-peer network, Mr. Kasnetz received a video file depicting minors engaged in sexually explicit conduct and the lewd and lascivious exhibition of the genitals of minors as defined by 18 U.S.C. § 2256.

4. The Indictment also alleges that on or about February 20, 2018, Mr. Kasnetz possessed material containing images and videos of child pornography, as described in 18 U.S.C. § 2256(8), that involved prepubescent minors and minors who had not attained 12 years of age on his HP Envy desktop computer, including four files described in the Indictment.

5. The child pornography described in the Indictment was discovered as a result of a search of Mr. Kasnetz' residence. In particular, on February 20, 2018, Judge Brandon Birmingham of the 292nd Judicial District Court, executed a Search Warrant, attached as Exhibit A, for Mr. Kasnetz's residence located at 9920 Strait Lane, Dallas, Dallas County, Texas.

6. The Search Warrant is supported by the Affidavit of Detective Chris DeLeon ("Affiant"), which was signed on February 20, 2018, and states in relevant part:

Between October 06, 2017 and November 02, 2017, Detective/TFO Jeff Rich, Plano Police Department, conducted an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated on October 6, 2017 for a device at IP address 70.122.154.184, because it was associated with a torrent with the infohash e95e98139e15a0b8dcbb485cbfb4959d3fc30c4a. This torrent file referenced 69 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running the investigative BitTorrent software, a direct connection was established with the device at IP address 70.122.154.184, hereinafter referred to as "Suspect Device".

Between Friday, October 06, 2017 and Thursday, November 02, 2017, hundreds of files of investigative interest to child pornography investigations were downloaded successfully that the device at IP address 70.122.154.184 was making available: The device at IP Address 70.122.154.184 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

After reviewing the files Affiant determined there to be hundreds of images and/or videos depicting children under the age of 18 years old engaged in sexual conduct in violation of Texas Penal Code 43.26, Possession or Promotion of Child Pornography, a felony.

See Exhibit A at ¶ 6.

III. GROUNDS FOR SUPPRESSION OF EVIDENCE

7. Defendant Kasnetz argues that the evidence obtained in this case as a result of the Search Warrant should be suppressed for the following reasons, which are in violation of the Fourth Amendment of the United States Constitution:

- a. The search was unreasonable and illegal because it was conducted without a valid search warrant and without probable cause, to-wit:
 - i. The discovery of the home address associated with the IP address was a warrantless and unreasonable search;
 - ii. Defendant Kasnetz had a legitimate expectation of privacy in transmissions routed from his device using BitTorrent, and the interception and analysis of Defendant Kasnetz's transmissions constituted an unlawful search and seizure;
 - iii. Information obtained by the unnamed "investigative BitTorrent software" was not in plain view;
 - iv. Use of the unnamed "investigative BitTorrent software" without prior judicial authorization constituted an unlawful search under the Electronic Communications and Protection Act and violated Defendant's reasonable expectation of privacy;
 - v. The information contained in the affidavit, taken as a whole, was insufficient to infer probable cause;
 - vi. The warrant was so lacking in indicia of probable cause, so as to render belief

in its existence, unreasonable, therefore it is not saved by the Leon exception, creating the good faith reliance rule;

- b. The items requested to be searched were seized in the illegal search of Defendant Kasnetz's transmissions and residence, and are therefore fruit of the poisonous tree.
- c. The evidence seized from Defendant Kasnetz's HP Envy desktop computer and other property was the result of an illegal search and seizure.
- d. Police officers during the search did not follow departmental protocol and turned off their bodycams.

IV. ARGUMENT

i. The Discovery of the Home Address Associated with the IP Address was a Warrantless and Unreasonable Search

8. While discovery of the IP Address 70.122.154.184 (and only the IP address) may not violate the Fourth Amendment, the State's use of a subpoena to obtain the physical location linked to the IP address was private information protected under the Fourth Amendment. Therefore, it was incumbent upon the State to use a warrant, not a subpoena, to obtain the home address. Because the State officers failed to seek a warrant before obtaining the home address, the warrant they subsequently obtained to search the home address was tainted. *See* Exhibit A at ¶ 6 ("Charter Communications was served with an administrative subpoena for subscriber information for account assigned to IP 70.122.154.184 on date/time aforementioned filed were downloaded.") The only source of the physical address was the IP address, therefore, the warrant fails to establish probable cause to search the home.

9. In *United States v. Weast*, 811 F.3d 743, 747–48 (5th Cir. 2016), the Fifth Circuit held that there is no reasonable expectation of privacy with respect to IP addresses, or images and information made publicly available in a shared folder on a peer-to-peer network. *Weast*, however,

predates the Supreme Court’s decision in *Carpenter v. United States*, in which the Supreme Court considered whether an individual has an expectation of privacy in cell-site location information (“CSLI”). 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018). The Supreme Court held that permitting government access to cell-site records without a warrant contravenes the Fourth Amendment expectation of privacy, and explained:

Cell phone location information is not truly “shared” as one normally understands the term. In the first place, cell phones and the services they provide are “such a pervasive and insistent part of daily life” that carrying one is indispensable to participation in modern society. *Riley*, 573 U.S., at —, 134 S.Ct., at 2484. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily “assume[] the risk” of turning over a comprehensive dossier of his physical movements. *Smith*, 442 U.S., at 745, 99 S.Ct. 2577.

Carpenter, 138 S. Ct. 2206, 2220, 201 L. Ed. 2d 507 (2018). *See State v. Mixton*, 247 Ariz. 212, 447 P.3d 829, 845 (Ct. App. 2019), *review granted* (Nov. 19, 2019) (Eckerstrom, J., concurring in part) (“As the majority observes, lower federal courts have consistently held that persons have no expectation of privacy in identifying information voluntarily conveyed to internet service providers. *See Weast*, 811 F.3d at 747-48; *Christie*, 624 F.3d at 573-74; *Perrine*, 518 F.3d at 1204. But my colleagues overlook that those cases pre-date, and have been overtaken by, the United States Supreme Court’s reasoning in *Carpenter*, 138 S. Ct. 2206.”).

10. Clearly, technological advancements now permit the government the ever increasing ability to monitor information that citizens consider private, and that this type of monitoring by the government requires a warrant. *See also United States v. Jones*, 565 U.S. 400, 403 (2012) (Sotomayor, J., concurring) (“GPS monitoring generates a precise, comprehensive

record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”).

11. In *Riley v. California*, the Supreme Court discussed at length whether the police could search a suspect’s cell phone data as part of his/her arrest, and concluded:

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans “the privacies of life,” *Boyd, supra*, at 630, 6 S.Ct. 524. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. **Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.**

Riley v. California, 573 U.S. 373, 403 (2014).

12. In light of *Carpenter* and other recent Supreme Court jurisprudence, such as *Jones* and *Riley*, it was incumbent upon the government to obtain a warrant to link an IP address to the subscriber’s name and physical address. There is nothing in the Affidavit to indicate that time was of the essence or that other factors precluded the government from taking this critical step.

ii. **Defendant had a Legitimate Expectation of Privacy in Transmissions Routed from his Device Using BitTorrent, and the Interception of Defendant’s Transmissions Constituted an Unlawful Search and Seizure Because It Captured Content**

13. The Search Warrant states that Defendant was using Bit Torrent, which the Search Warrant describes as follows:

BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link

to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file.

To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

See Exhibit A at ¶ 6. By using BitTorrent, Defendant Kasnetz agreed to BitTorrent's End User Licensing Agreement, and to the exchange of torrent files with other users of the BitTorrent software. Defendant Kasnetz' acceptance of BitTorrent's End User Licensing Agreement confirms his intent to exchange torrent files only with other individuals who also had entered into BitTorrent's End User Licensing Agreement and who would be matched by the BitTorrent software. In fact, the Affidavit itself supports this as it states:

For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and **share files from their device with other BitTorrent users.** Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. . . .

To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. **The BitTorrent software** processes the information in the torrent file and **locates devices on the BitTorrent network** sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after **the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.**

See Exhibit A at ¶ 6 (emphasis added).

14. In contrast, Detective Rich was not using Bit Torrent. Rather, Detective Rich was using an unnamed "investigative Bit Torrent software," which unlike BitTorrent, enabled him to make a direct connection to Defendant Kasnetz's computer:

Between October 06, 2017 and November 02, 2017, Detective/TFO Jeff Rich, Plano Police Department, conducted an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated on October 6, 20 17 for a device at IP address 70.122.154.184, because it was associated with a torrent with the infohash e95e98139e15a0b8debb485cbfb4959d3fc30c4a. This torrent file referenced 69 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running the investigative BitTorrent software, a direct connection was established with the device at IP address 70.122.154.184, hereinafter referred to as "Suspect Device".

Between Friday, October 06, 2017 and Thursday, November 02, 2017, hundreds of files of investigative interest to child pornography investigations were downloaded successfully that the device at IP address 70.122.154.184 was making available:. The device at IP Address 70.122.154.184 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

See Exhibit A at ¶ 6.

15. Significantly, nowhere does the Affidavit allege that the unnamed “investigative BitTorrent software” was Peer to Peer (“P2P”) software. In fact, the Search Warrant purposefully fails to identify the “investigative” software being used by Detective Rich as Detective Rich and/or Affiant Detective DeLeon obviously knows the name of the software or readily could obtain such information. Regardless, the Affidavit is clear: Detective Rich was not using BitTorrent.

16. Because Detective Rich was not using BitTorrent or other P2P software, he was neither a party to BitTorrent’s End User License Agreement, nor was he someone with whom Defendant Kasnetz had agreed or intended to exchange torrent files. As such, Detective Rich was a usurper of BitTorrent’s system, not a user.

17. “The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” *Katz v. United States*, 389 U.S. 347, 351 (1967). “But **what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.**” *Id.*

(emphasis added). *See also United States v. Jones*, 565 U.S. 400, 403 (2012) (excluding GPS evidence recording publicly observable information about vehicle location on Fourth Amendment grounds). “[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” *Kyllo v. United States*, 533 U.S. 27, 33 (2001), citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

18. In *United States v. Jones*, the Supreme Court addressed whether police use of a GPS tracking device required a warrant. The Government had “installed a GPS tracking device on the undercarriage of the [defendant’s] Jeep while it was parked in a public parking lot.” 565 U.S. at 403. “Over the next 28 days, the Government used the device to track the vehicle’s movements, and once had to replace the device’s battery when the vehicle was parked in a different public lot in Maryland.” *Id.* “By means of signals from multiple satellites, the device established the vehicle’s location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer.” *Id.* “It relayed more than 2,000 pages of data over the 4-week period.” *Id.*

19. Although Justice Scalia’s majority opinion in *Jones* focused on the police placement of the device as a trespass, Justices Alito and Sotomayor each authored a concurrence focused on the idea that monitoring an individual’s location over time is an invasion of privacy on its own. In Justice Sotomayor’s concurrence, she stated that she would “take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements.” *Id.* at 416 (Sotomayor, J., concurring) (“I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on”). In addition, Justice Sotomayor stated that:

it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information

voluntarily disclosed to third parties. *E.g., Smith*, 442 U.S., at 742, 99 S.Ct. 2577; *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

United States v. Jones, 565 U.S. at 417–18 (emphasis added). *See also Florida v. Jardines*, 133 S. Ct. 1409, 1411-12 (2013) (Kagan, J., concurring) (arguing that in considering whether police use of drug sniffing dog at the front door of a home constitutes a search under the Fourth Amendment, the Court must consider privacy issues, not just property issues, because people have a heightened expectation of privacy in their homes and the areas immediately surrounding their homes, which the police had violated).

20. Here, Defendant Kasnetz did not expose torrent files to the public. Rather, he used the BitTorrent network, which is designed to maintain anonymity, and therefore, manifests Defendant Kasnetz’s actual and subjective expectation of privacy. Under the circumstances, Defendant Kasnetz had an actual and subjective belief that the communications and content sent from and routed through his electronic device would be private. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (“we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP.”) (internal quotation omitted); *Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 970 (11th Cir. 2016) (agreeing with *Warshak* and holding “that the Fourth Amendment demands that the government demonstrate probable cause both to intercept real-time wire, oral, and electronic communications and to review the content of stored electronic communications”); *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (holding that the interception of e-mail messages that had already

been sent and were in “transient electronic storage,” such as on a hard drive or in RAM, constitutes an “interception” under Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, and a criminal offense).

21. Further, Defendant Kasnetz’ subjective expectation of privacy in Bit Torrent communications and content is one that society recognizes as reasonable. As stated by Justice Sotomayor in *Jones*:

I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disintitiled to Fourth Amendment protection. See *Smith*, 442 U.S., at 749, 99 S.Ct. 2577 (Marshall, J., dissenting) (“Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes”); see also *Katz*, 389 U.S., at 351–352, 88 S.Ct. 507 (“[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected”).

United States v. Jones, 565 U.S. at 418 (emphasis added).

22. Similarly, Judge Eckerstrom’s recent concurrence in *State v. Mixton*, states:

our actions on the internet expose our worries, fantasies, and political views at least as comprehensively as the sequence of our physical locations. Internet access has likewise become an integral part of participation in contemporary culture: it is a place we shop, converse with friends and romantic partners, seek information about medical conditions, and debate the issues of the day. And, as with cell-phone use, one cannot secure such access without exposing some private information to a vendor. See *Carpenter*, 138 S. Ct. at 2220 (questioning whether persons voluntarily “assume[] the risk” of exposing private actions under such circumstances (alteration in *Carpenter*) (quoting *Smith*, 442 U.S. at 745, 99 S.Ct. 2577)).

In fact, our expectation of privacy in internet use is arguably greater than any similar expectation we hold for our physical movements in public. A visit to an internet site is presumptively anonymous unless we choose to make it otherwise; our movements on public streets are presumptively visible to all we encounter. For this reason, the Court has required a warrant for the locational tracking of criminal suspects only when that tracking is sufficiently protracted to reveal private features of their lives. *See, e.g., id.* at 2220; *United States v. Jones*, 565 U.S. 400, 430, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). By contrast, each discrete internet visit may expose an acutely private thought process and may do so in a context where the visitor has taken every precaution to retain his anonymity. Surely, if the government is required to obtain a warrant to track, through technology, a suspect’s public physical movements, it should likewise need a warrant to expose a suspect’s private digital behavior.

Mixton, 447 P.3d at 846 (emphasis added).²

23. Moreover, the Government’s use of this technology cannot be said to be excepted under the Third Party Doctrine because the Government was capturing content. *See Smith v. Maryland*; *Carpenter*, *supra*. Here the Government was intercepting not just “innocuous” metadata. Rather, the Government was intercepting *content* as evidenced by the officer’s Affidavit regarding the very content downloaded. Any averment by the Government otherwise is without merit.

² Omitted note 13 of Judge Eckerstrom’s concurrence states:

As my dissenting colleague correctly observes, many people choose to use the internet for public activities, such as social media, wherein they consciously relinquish any expectation of privacy. But, as Judge Posner has explained, an expectation of privacy is not an expectation of total secrecy. Posner, *supra* ¶ 24, at 342. Rather, it is an expectation that a person has the power to selectively determine who may have access to a presumptively private domain. We do not waive our right of privacy in our homes simply because we occasionally choose to invite relatives, friends, or housekeepers to enter it. Similarly, we do not waive our right of privacy in all our internet activities simply because we choose to make some part of it public.

Mixton, 447 P.3d at 846 n.13.

24. In sum, Defendant Kasnetz had a legitimate expectation of privacy in transmissions routed from his device using BitTorrent, as demonstrated by his decision to not only use BitTorrent, but also his acceptance of the BitTorrent End User Licensing Agreement. Because Detective Rich admittedly was not a user or participant of BitTorrent, he was not an intended recipient of any files transmitted by Defendant Kasnetz. The purposeful interception of these transmissions by a non-user employing the unnamed “investigative BitTorrent” program constituted an unlawful search and seizure.

**iii. Information Obtained by the Unnamed
“Investigative BitTorrent Software” was not in Plain View**

25. The Search Warrant states that Detective Rich was using unnamed “investigative Bit Torrent software.” *See* Exhibit A at ¶ 6. Defendant Kasnetz anticipates that the government may raise the “plain view” exception in defense of its warrantless search. In order for the plain view exception to apply, three requirements must be satisfied: i) the officer’s intrusion into the location where the evidence is located must be lawful, ii) the discovery of the evidence must be inadvertent, and iii) the incriminating nature of the evidence must be immediately apparent. *See Texas v. Brown*, 460 U.S. 730, 793 (1983).

26. As described in the affidavit, Detective Rich targeted the suspect device at IP address 70.122.154.184, because it “was associated with the infohash d950b8debbb485cbfb4959d3fc30c4a,” which “referenced to 69 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.” *See* Exhibit A at ¶ 6. Based on the info hash of the torrent file, Detective Rich assumed that the suspected machine had downloaded child pornography. (Incidentally, even though the discovery of this file serves as the foundation for the State’s actions, the Affidavit fails to provide any information regarding why the file was of “investigative interest.”)

27. Turning to the Affidavit in support of the search warrant, the BitTorrent software acts as a matchmaker between users:

To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

See Exhibit A at ¶ 6. Defendant Kasnetz was using BitTorrent.

28. In contrast, Detective Rich used unnamed “investigative BitTorrent software” to track down a file of “investigative interest to child pornography investigations,” then specifically targeted the source of the file:

Using a computer running the investigative BitTorrent software, a direct connection was established with the device at IP address 70.122.154.184, hereinafter referred to as "Suspect Device".

Between Friday, October 06, 2017 and Thursday, November 02, 2017, hundreds of files of investigative interest to child pornography investigations were downloaded successfully that the device at IP address 70.122.154.184 was making available. The device at IP Address 70.122.154.184 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

See Exhibit A at ¶ 6. The plain language of the Affidavit undermines the probable cause façade it attempts to convey: the unnamed “investigative BitTorrent software” was not part of the BitTorrent user network, but rather a surreptitious hunter who, disguised as a BitTorrent network user, specifically targeted a device using BitTorrent.

29. Therefore, the government cannot take cover under the plain view exception. The intrusion into Defendant Kasnetz’ transmissions and/or device was unlawful, and there was nothing inadvertent about the government’s discovery of the evidence at issue.

iv. Use of the Unnamed BitTorrent Investigative Software Without Prior Judicial Authorization Constituted an Unlawful Search Under the Electronic Communications and Protection Act and Violated Defendant’s Reasonable Expectation of Privacy

30. The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510-2523. The ECPA as amended, protects wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers. *See* <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>. The Act applies to email, telephone conversations, and data stored electronically. *Id.* *See also* 18 U.S.C. §§ 2510–22.

31. Both ECPA and the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2712, require that law enforcement go through appropriate application and affidavit procedures before a judge can enter an ex parte order authorizing or approving interception of wire, oral, or **electronic communications** or retrieval of stored electronic communications. *See* 18 U.S.C. § 2518(1) -(3) (emphasis added). Pursuant to the ECPA, an “application for an order authorizing or approving the interception of a wire, oral, or electronic communication...shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application.” 18 U.S.C. § 2518(1) (emphasis added). Section 2518 also sets forth the information required to be contained in each application under the ECPA to enable the judge to determine whether there is probable cause for intercepting the communication. *See* 18 U.S.C. § 2518(1), (3). No such order was sought in this case before law enforcement intercepted and stored communications.

32. In addition, per the ECPA, the term “‘intercept’ means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). Further, per the ECPA, the term “‘contents’, when used with respect to any wire, oral, or electronic communication, includes any information

concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8). Moreover, an “electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce,” outside of some specified exceptions that are inapplicable here. 18 U.S.C. § 2510(12).

33. Here, Detective Rich was utilizing a program (i.e., the unnamed “investigative BitTorrent software”) that had been modified for law enforcement to log the IP address and torrent info hash being transmitted. *See* Exhibit A at ¶ 6. This data unquestionably constituted “electronic communications” under 18 U.S.C. § 2510. Detective Rich intercepted the data by logging it through use of the unnamed “investigative BitTorrent software.” He then acquired the content of the transmissions at issue and used that content to match files’ identifying data (“info hash”) to known files, stored the data he had intercepted, then utilized the unnamed “investigative BitTorrent software” to access the actual files. *See* Exhibit A at ¶ 6.

34. At no time did Detective Rich apply for authorization to intercept such information, as described in 18 U.S.C. § 2518(1), and at no time did law enforcement possess a warrant for such a search. Because the Affidavit fails to establish that the unnamed BitTorrent investigative software shared files or pieces of files as is required for users of the Bit Torrent network, Detective Rich and the unnamed BitTorrent investigative software were never a party to the communications. 18 U.S.C. § 2511(2)(a) and (c) (“It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception”) (emphasis added). Law enforcement likewise appears to have failed to request authorization to access the electronic communications stored by the unnamed BitTorrent

investigative software, in violation of the Stored Communications Act, 18 U.S.C. §§ 2701-2712.

35. While ECPA itself contains no exclusionary provision for such illegally intercepted information, suppression of the information obtained through law enforcement's interception of data using the unnamed BitTorrent investigative software is proper. Congress recognized Defendant's legitimate expectation of privacy in such communications by enacting ECPA and specifically protecting the privacy of those communications and penalizing violations as felony offenses under 18 U.S.C. § 2511. Defendant likewise intentionally availed himself of additional protection by using the Bit Torrent network to make his electronic communications even more private and anonymous.

36. The general exclusionary rule under the Fourth Amendment applies to require that the evidence obtained by law enforcement in violation of Defendant's subjective expectations of privacy, an expectation that has been recognized as reasonable by society and that is reflected in Congress' legislation in ECPA, was violated by law enforcement's interception, storage, search and seizure of Defendant's electronic communications and/or those of his computer in this case and all evidence seized in this case should be suppressed.

**v. The Information Contained in the Affidavit, Taken as a Whole,
was Insufficient to Infer Probable Cause**

37. "No warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Thus, the Constitution is clear that a magistrate may issue a search warrant for a location only if the Affiant establishes in the affidavit probable cause to believe evidence of a crime may be found there. Probable cause exists when, under the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (affidavit must provide "substantial

basis” for determining probable cause).

38. In so doing, the Court must consider the supporting affidavit and whether “[s]ufficient information” was “presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.” *Gates*, 462 U.S. at 239. *See also United States v. Barrington*, 806 F.2d 529, 532 (5th Cir. 1986) (“bare bones affidavits are inadequate”); *Florida v. Harris*, 133 S. Ct. 1050, 1056 (2013) (“We have rejected rigid rules, bright-line tests, and mechanistic inquiries in favor of a more flexible, all-things-considered approach.”)

39. With regard to timeliness, the Fifth Circuit has held that “[t]he amount of delay which will make information stale depends upon the particular facts of the case, including the nature of the criminal activity and the type of evidence sought.” *United States v. Allen*, 625 F.3d 830, 842 (5th Cir. 2010) (citing *Bastida v. Henderson*, 487 F.2d 860, 864 (5th Cir.1973)).

40. In *Allen*, the court rejected the defendant’s staleness argument, because the court found that the affidavit contained not only generalized allegations (i.e., that computers can store digital images indefinitely and that remnants of files can be recovered “months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet”), but also assertions specific to Allen, including that “because of the fact that Allen appears to have traded images depicting child pornography and engaged in chat sessions discussing the trade of child pornography, the agent believed Allen had a sexual interest in children.” *Allen*, 625 F.3d at 843.

41. The *Allen* court also relied on other cases which held that particularized facts were key factors which weighed against staleness concerns. *Id.* 843-844. *See United States v. Riccardi*, 405 F.3d 852, (10th Cir. 2005) (information that suspect called teen boys for gratification and possessed 300 photographs of children was enough to support belief that evidence would be found

on his computer); *United States v. Frechette*, 583 F.3d 374, 379 (6th Cir. 2009) (among facts known to officer was that defendant was a convicted sex offender); *United States v. Lacy*, 119 F.3d 742, 745–46 (9th Cir. 1997) (defendant had called to order pornography on 16 occasions); *United States v. Paull*, 551 F.3d 516, 522 (6th Cir.2009) (affidavit stated that defendant had subscribed to child pornography websites and that he continued to do so over the course of two years); *United States v. Morales-Aldahondo*, 524 F.3d 115, 117 (1st Cir. 2008) (defendant was among the five largest-volume purchasers from pornography distributor); *United States v. Newsome*, 402 F.3d 780, 783 (7th Cir. 2005) (in addition to eyewitness account that defendant had, a year before, had pornographic images of children, magistrate knew that defendant had “recently” had video of child taped with hidden camera).

42. Here, the Search Warrant was issued on February 20, 2018, based upon events described in the Affidavit as occurring months earlier between October 6, 2017 and November 2, 2017. The Affidavit contains generalized allegations about the penchant of child pornography offenders to amass collections, share child pornography, and store child pornography in electronic form because it is “inexpensive” and “readily accessible” for viewing and sharing. *See* Exhibit A at ¶ 17. The Affidavit further describes how some individuals “rarely, if ever, dispose of their illicit materials,” while “[o]thers routinely collect and then delete their collections out of fear of detection or remorse only to later re-acquire them.” *Id.* In sum, the Affidavit is long on assumptions and generalizations, but short on specifics. In fact, the Affidavit contains no allegations specific to Defendant Kasnetz which might support probable cause to believe that despite the passage of time, Defendant Kasnetz would have retained images on his computer, such as a subscription to a child pornography site, online chats about child pornography, past criminal behavior, or the like. Without facts demonstrating that Kasnetz, in particular, traded and was the

sort of person who would retain, pornographic images, the affidavit rested on the assumption that all “collectors of child pornography keep their materials indefinitely.” *See Lacy*, 119 F.3d at 746 (stating court was unwilling to make such an assumption). Because that assumption is insufficient to provide probable cause that Kasnetz, as opposed to a generic possessor of child pornography, retained images on his computer, the evidence must be suppressed.

vi. The warrant was so lacking in indicia of probable cause, so as to render belief in its existence, unreasonable, therefore it is not saved by the Leon exception, creating the good faith reliance rule

43. The good faith exception to the probable cause requirement cannot be applied here. *See United States v. Leon*, 468 U.S. 897 (1984) (officer’s good faith reliance on magistrate’s determination of probable cause will protect action from exclusionary rule). That exception has no force where, as here, an officer obtains a warrant and conducts a search based on the inadequate information he himself provides to a magistrate. *See United States v. Barrington*, 806 F.2d 529, 532 (5th Cir. 1986). Moreover, “[a] warrant based on an affidavit that is obviously insufficient to establish probable cause does not justify an officer’s reliance.” *United States v. Davis*, 226 F.3d 346, 351 (5th Cir. 2000). In particular, the Affidavit contains misstatements and omissions designed to obfuscate the issues and mislead the issuing judge, including:

- a. Failure to identify the “investigative BitTorrent software” as described more fully above;
- b. Failure to specify whether the unnamed “investigative BitTorrent software” was operating as P2P software;
- c. Implying that in using the unnamed “investigative BitTorrent software” Detective Rich was participating in the BitTorrent network, when he was not;

- d. Failing to include allegations specific to Defendant Kasnetz which might support probable cause to believe that despite the passage of time, Defendant Kasnetz would have retained images on his computer, such as a subscription to a child pornography site, online chats about child pornography, past criminal behavior, or the like;

44. In sum, the Affidavit is short on particulars, but long on filler. Law enforcement relied on fluff to mislead the issuing judge because they lacked specifics and with each passing day the investigation became more temporally remote. In this regard, *Allen* and all of the cases discussed therein put the officers on notice that the Affidavit lacked probable cause. 625 F.3d at 843-844.

V. CONCLUSION

WHEREFORE, Defendant Andrew Kasnetz prays this Honorable Court will grant an evidentiary hearing and thereafter suppress from use at trial any and all evidence obtained after the warrantless use of the “investigatory BitTorrent software” in this matter.

Respectfully submitted,

/s/ Connor Nash

Connor Nash

State Bar No. 24116809

Email: connor@nashpllc.com

NASH LAW, PLLC

2975 Blackburn, #1419

Dallas, Texas 75204

Telephone: (214) 395-9504

ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I certify that a true copy of the above was served on each attorney of record in accordance with the Federal Rules of Criminal Procedure.

/s/ Connor Nash
Connor Nash

EXHIBIT A

AFFIDAVIT FOR SEARCH WARRANT

STATE OF TEXAS
COUNTY OF DALLAS

§
§

9920 Strait Lane
Dallas, Texas

COMES NOW, undersigned Affiant, Detective Chris DeLeon, #8889, being a Peace Officer under the laws of Texas and being duly sworn, on oath makes the following statements and accusations:

- 1) There is a suspected place and premises 9920 Strait Lane, Dallas, Dallas County, Texas. Said premises is a single family residence located behind a light brown brick wall with a gate securing access through the driveway. The numbers "9920" are affixed to the left side of the driveway in dark numbering on a dark background above a call box. Dallas Appraisal District identified the legal description as BLK A/5544, LT 4 ACS 0.950, 9920 Strait Ln., Dallas, Texas.
- 2) Said premises, in addition to the foregoing description, also includes all other buildings, structures, places and vehicles on said premises and within the curtilage, if said premises is a residence, which are found to be under the control of the SUBJECT(s) named herein, and in, on, or around which said SUBJECT(s) may reasonably repost or secrete property which is the object of the search requested herein.

The place and premises, herein PREMISES, is further described in Attachment A, which is incorporate into this affidavit by reference.

- 3) There is at said place and premises the following item(s) which are property the possession of which is prohibited by law, implements or instruments used in the commission of a crime in violation of the laws of the State of Texas, property or items constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense, to wit:
 - a. Child pornography.
 - b. Visual materials and other items of child erotica.
 - c. Information and records pertaining to the access, display, possession, or distribution of child pornography and child erotica.
 - d. Information and records pertaining to the search, research, and correspondence regarding the subject matter of child pornography and child erotica.
 - e. Information and records that would tend to establish that a computer, computer system, computer network, electronic storage device, cellular telephone, or other wireless communications device was used to search, solicit, access, display, possess, or distribute child pornography and establish the person(s) who used, control, or own said device or system.
 - f. Account information, passwords, keys, encryption keys, and other materials required to gain access to containers or devices having the information and records sought in this affidavit.
 - g. Information and records pertaining to sexual conduct with a minor or the sexual assault of a minor.
 - h. Items used to engage in sexual conduct with a minor or the sexual assault of a minor.

- i. Records and items which manifest ownership, dominion, or occupancy over the PREMISES, vehicles, storage areas, safes, out buildings, and containers being searched to include letters, utility bills, telephone bills, mail envelopes, mortgage/lease documents, credit card documents, receipts, articles of personal property, keys, and photographs of the SUBJECT(S) and his/her associates.
 - j. Computers, computer systems, electronic storage devices, cellular phones, and other wireless communication devices that may contain the information and records sought in this affidavit or may have been used in the commission of the alleged offense(s).
 - k. Electronic communications held or maintained in electronic storage by an electronic communication service or remote computing service associated with any computer, computer system, electronic storage device, cellular phone, or other wireless communications device searched or seized pursuant to this affidavit that may contain the information and records sought in this affidavit or may have been used in the commission of the alleged offense(s).
- 4) Said suspected place and premises and personal property are in charge of and controlled by each of the following persons:
- Andrew Kasnetz (W/M, 03-30-1964) and/or others unknown to the Affiant.
- 5) It is the belief of Affiant who hereby charges and accuses that persons unknown to Affiant at this time committed the offense of Possession or Promotion of Child Pornography as defined by PC , 43.26.
- 6) The facts establishing Affiant's basis for probable cause for the issuance of a warrant are as follows:

I, your Affiant, Detective Chris DeLeon, #8889, of the Dallas Police Department, am currently assigned to the Specialized Investigations Division, Internet Crimes Against Children Unit located at 1400 S. Lamar St. Dallas, Dallas County, Texas. Affiant is responsible for the investigation of non-familial child molestation and sexual assault cases, child pornography and other offenses involving the exploitation of children having a technological nexus. I have been a Texas peace officer since August 2006.

Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file.

To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is

achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

Between October 06, 2017 and November 02, 2017, Detective/TFO Jeff Rich, Plano Police Department, conducted an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated on October 6, 2017 for a device at IP address 70.122.154.184, because it was associated with a torrent with the infohash e95e98139e15a0b8debb485cbfb4959d3fc30c4a. This torrent file referenced 69 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running the investigative BitTorrent software, a direct connection was established with the device at IP address 70.122.154.184, hereinafter referred to as "Suspect Device".

Between Friday, October 06, 2017 and Thursday, November 02, 2017, hundreds of files of investigative interest to child pornography investigations were downloaded successfully that the device at IP address 70.122.154.184 was making available. The device at IP Address 70.122.154.184 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

After reviewing the files Affiant determined there to be hundreds of images and/or videos depicting children under the age of 18 years old engaged in sexual conduct in violation of Texas Penal Code 43.26, Possession or Promotion of Child Pornography, a felony.

One file reviewed by Affiant was "pthc_ptsc_9yo jenny in nylons and collar tied up" and found it to be an image depicting a prepubescent female child engaged in sexual conduct. Specifically, the child is tied up on a bed in a manner exposing her vagina and chest nude except for black stockings.

Another file reviewed by Affiant was "! New ! (Pthc) Tara 8Yr - Tara Gets Molested By A Clown(taraPart 1)" and found it to be a 12 minute 56 second video depicting a prepubescent female child engaged in sexual conduct. Specifically, the female child is positioned on a bed nude except a mask while an adult male inserts his fingers and a sex toy into the child's vagina, has the child perform oral sex on him and inserts his penis into the child's vagina.

Charter Communications was served with an administrative subpoena for subscriber information for account assigned IP 70.122.154.184 on date/time aforementioned files were downloaded. Charter Communications' response identified account 8260132080835662 with listed subscriber Andrew Kasnetz and a service address of 9920 Strait Lane, Dallas, TX 75220.

Texas Drivers License 00850762 lists Andrew Kasnetz's home address as 9920 Strait Lane, Dallas, Texas 75220.

A 2014 black Ford Explorer (Texas Tag DNW0226) and a 2015 black Mercedes SL63 AMG (Texas Tag FLK7971) show to be owned by Andrew Kasnetz. The Ford registration lists a home address of 9920 Strait Lane, Dallas, Texas 75220. The Mercedes lists a home address of PO BOX 190543, Dallas, TX 75219.

Officers with Dallas Police Department's Fugitive Task Force conducted surveillance of Premise on February 12, 2018. A Ford Explorer bearing Texas Tag DNW0226 arrived at Premise at approximately 4:50 pm.

7) Definitions

Affiant uses the following terms to convey the following meanings:

- a) "Child pornography" means visual material that visually depicts a child younger than 18 years of age at the time the image of the child was made who is engaging in sexual conduct, including a child who engages in sexual conduct as a victim of an offense under Section 20A.02(a)(5), (6), (7), or (8) of the Texas Penal Code.
- b) "Computer", as defined in Texas Penal Code 33.01(4), means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.
- c) "Computer network", as defined in Texas Penal Code 33.01(5), means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.
- d) "Computer system", as defined in Texas Penal Code 33.01(8), means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.
- e) "Data", as defined in Texas Penal Code 33.01(11), means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punch cards, or may be stored internally in the memory of the computer.
- f) "Electronic Storage Device" means any device or medium capable of storing data that can be readily accessed by a computer. This includes hard drives; solid state drives; flash memory devices such as USB drives and memory cards; optical media such as CD, DVD, and Blu-ray disks; devices with internal memory such as a cellular telephone or camera; volatile computer memory; et cetera. Such devices may overlap with the definition of a computer.
- g) "Sexual conduct", as defined in the Texas Penal Code 42.25(2), means sexual contact, actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals, the anus, or any portion of the female breast below the top of the areola.
- h) "Visual Material", as defined in Texas Penal Code 43.26(b)(3), means any:
 - A. film, photograph, videotape, negative, or slide or any photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide; or
 - B. any disk, diskette, or other physical medium that allows an image to be displayed on a computer or other video screen and any image transmitted to a computer or other video screen by telephone line, cable, satellite transmission, or other method.

8) Seizure of Computers and Electronic Storage Devices

Affiant requests permission to search and seize the sought records and information that may be found on the PREMISES in whatever form they are found. Affiant submits that if a computer or electronic storage device is found on the PREMISES, there is probable cause to believe those records and information sought will be stored in that computer or electronic storage device. This is due to the increasing tendency to store and transmit documents in electronic form, engage in communication by electronic means, and the nature of the alleged offense(s) which directly employs computers, computer systems, computer networks, and electronic storage devices in the commission of the alleged offense(s). Furthermore, the records and information sought are likely

to remain on computers and electronic storage devices for months or even years after the last act in the commission of the alleged offense(s) is committed.

To the extent necessary to completely and accurately retrieve data maintained in a computer or electronic storage device, Affiant requests permission to search and seize all seized devices' peripherals; exterior and removable storage devices; related instructions in the form of manuals and notes; and, in the case of computers, the computer system as a whole.

It is often necessary to take all seized devices and related equipment/materials to a qualified computer specialist in an appropriate setting in order to ensure the accuracy and completeness of the search and to prevent the loss of data either from accidental or intentional destruction. To that end, your Affiant requests permission to transport any computers or electronic storage devices seized pursuant to this affidavit to an off-site location, to include a location outside of the County where the seizure occurs, to have forensic analysis conducted on these items

Because several people may share the PREMISES, it is possible that the PREMISES will contain computers and electronic storage devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If officers conducting the search nonetheless determine that it is possible that evidence described in this affidavit could be found on those computers and devices, Affiant seeks permission to search and if necessary to seize those computers and devices as well. It may be impossible to determine, on scene, which computers and electronic storage devices contain the items of evidence described in this affidavit.

9) Forensic Examination of Computers and Electronic Storage Devices

Searching computer systems, to include cellular phones, for the property, evidence, and items described in this affidavit may require a range of data analysis techniques. In some cases, it is possible for officers and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the affidavit. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require officers or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the affidavit. In light of these difficulties, Affiant requests authorization to use whatever data analysis techniques appear necessary to locate and retrieve the property, evidence, and items sought in this affidavit.

10) Cellular Phones & Wireless Communication Devices

Through Affiant's knowledge, training, and experience, Affiant knows that cellular telephones and other wireless communication devices are fundamentally computers and are generally capable of acting as electronic storage devices. Furthermore, they are capable of connecting to computer networks, including the Internet, via cellular radio and/or Wi-Fi.

Having established probable cause to search and seize computers and electronic storage devices, Affiant requests authorization to search and seize all cellular telephones and other wireless communication devices found on the PREMISES belonging to the SUBJECT(s) and other occupant(s) of the PREMISES.

11) Networking Equipment

Networking equipment such as modems, routers, wireless access points, et cetera may contain the evidence sought in this affidavit in the way of logs, MAC address, network configuration information, and Wi-Fi configuration. In addition, this equipment is part of the computer system as a whole.

Affiant requests authorization to seize networking equipment found at the PREMISES pursuant to the probable cause already established for seizure of computers, computer systems, and electronic storage devices.

12) Electronic Data Held in Remote Storage

Information on the device may include electronic communications held or maintained in electronic storage by an electronic communication service or remote computing service, as those services are defined within 18 U.S.C. 2703. This type of communications may be stored in the SUBJECT(s)' device or other electronic devices in the form of e-mail, instant message chats, and any other type of other related electronic communication. This specific federal law noted above, which is part of the Electronic Communications Privacy Act, allows interception of such electronic communication pursuant to a search warrant for which the grounds for issuance are established under the Texas Code of Criminal Procedure Articles 18.02, 18.20, and 18.21 et seq.

Affiant requests authorization to access said communications that are found to be associated with any computer, computer system, computer network, cellular telephone, or other wireless communication device which may contain the information and records sought in this affidavit.

13) IP Address

An Internet Protocol address (IP address) is a value assigned to a device participating on a network utilizing Internet Protocol. It serves as a device identifier and establishes a location on the network. IP addresses are used for devices connected to the Internet as well as devices connected to private networks such as home networks, corporate networks, government networks, et cetera.

Each device connected to the Internet is assigned an IP address often referred to as the device's public IP address. Many devices share a common public IP address through a router which acts as a bridge between the Internet and private networks. The devices participating on the private network pass communications to the Internet through their router having the public IP address.

Devices communicate with each other by addressing messages with the intended recipient's IP address. Messages sent over the Internet to devices on a private network are addressed to the public IP address of the private network's router. Once received by the router, the messages are forwarded to devices on the private network based on the configuration of the router.

Ranges of public IP addresses are assigned to specific entities which in turn often assign specific IP address to other entities. These entities are generally able to provide details about a specific IP address within their assigned range such as subscriber information or physical location of the device or router utilizing the public IP address.

Information about devices on a private network such as location, identity, or whether it is the origin or recipient of some communication over the Internet can only be determined by examining the private network and its connected devices.

14) Hash Functions

A hash function is a mathematical algorithm which, for a given input of data, produces a fixed length output called the hash value. Hash values are commonly used in computer science as unique identifiers or "fingerprints" for data such as a file.

The hash value can be further described as:

A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. "Hashing" is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

15) Peer-to-Peer File Sharing

Peer-to-peer file sharing networks allow users to receive (download) and send (upload) files across the Internet using generally free software and an Internet connection. Each file sharing network has different network topology, protocols, et cetera, but each fundamentally allows the computers of each end user to communicate directly with one another to send and receive files. This is in contrast to the more traditional client-server model where clients receive files from a centralized server.

Peer-to-peer file sharing networks have grown in popularity serving as efficient means to distribute files. However, some files shared over these networks are illicit and child pornography is known to be shared across these networks.

16) BitTorrent

BitTorrent is a communications protocol to enable peer-to-peer file sharing over the Internet. Any computer running software which conforms to the BitTorrent protocol is able to participate on the BitTorrent network. Such software is referred to as the BitTorrent client and examples include µTorrent, Vuze, Deluge, and BitComet. BitTorrent clients are readily and freely available on the Internet and device app stores for multiple platforms (PCs, servers, smartphones, tablets, etc.) and operating systems.

Files shared across the BitTorrent network are shared as a collection containing a single file or multiple files which can be of any file type. The BitTorrent protocol specifies a means of dividing collections into conceptually separate pieces. This allows clients to download different pieces of the same collection simultaneously from different users, known as peers. It also enables clients in the processes of receiving a collection to simultaneously send the pieces it has already acquired to another peer attempting to acquire the same collection before the client has obtained all the pieces of the collection.

17) Child Pornography Offenders

Affiant is aware through experience and training, as well as conversations with other law enforcement officers trained and experienced in this area, that the majority of individuals who intentionally access and possess child pornography are persons who are sexually attracted to children. They are sexually stimulated and receive sexual gratification from sexual fantasies involving children and visual depictions of children that are sexual in nature.

These individuals generally prefer to store child pornography in electronic form on computers and electronic storage devices. This allows for the inexpensive storage of large collections of child pornography which are

readily accessible to a computer for viewing, replication, and sharing with others via the Internet or other computer network.

These individuals typically collect multiple images and/or videos of child pornography and these collections are generally in excess of what is initially detected by law enforcement. Many of these individuals amass large collections of child pornography and rarely, if ever, dispose of their illicit materials. Others routinely collect and then delete their collections out of fear of detection or remorse only to later re-acquire them. However, deleted files on computers or electronic storage devices do not necessarily cause the data to be removed from the device and can be recovered through forensics analysis.

These individuals often store child pornography on more than one computer or electronic storage device. Data is easily moved between different devices and those who possess child pornography have compelling reasons to do so, such as avoiding detection by transferring materials from a shared device to a private device; copying materials to multiple devices for convenient access; transferring materials to a device that can be transported and accessed outside their residence; and duplication for the purposes of backing up their collection. In addition, many individuals utilize remote storage (cloud storage) providers such as Dropbox, Box.com, Google Drive, and others as a means to store and access their collections from any device with an Internet connection.

There are multiple means of obtaining child pornography on the Internet such as websites, hidden Tor services, peer-to-peer filing sharing networks, discretely disseminated links to materials held in cloud storage, email, instant message (chat) services, et cetera. These individuals generally utilize more than one source to obtain child pornography. They also use websites and correspond with one another to discover available sources of child pornography, research topics relevant to child pornography, and seek to understand and validate their sexual interest in children. Many also trade child pornography through the Internet with individuals or online communities with which they have developed a relationship in addition to more anonymous means such as public peer-to-peer networks.

In addition to child pornography, these individuals often have collections of child erotica. These are materials or items that are sexually arousing to persons having a sexual interest in children, but are not necessarily obscene or do not necessarily depict children in sexually explicit poses or positions. Examples include non-nude images of children in swimsuits, the non-nude photographs belonging to set of child pornography photographs, cartoon drawings of children having sexual intercourse, written stories about seducing children, and so forth. The possession of child erotica is material evidence as it may corroborate other evidence that shows that a particular person is in possession of child pornography, support the assertion that particular person has a sexual interest in children, and demonstrate a person's intent in possessing child pornography.

18) Search of Persons and Vehicles

Affiant requests permission to enter and search any vehicles found at or connected to this PREMISES or any vehicles found at the PREMISES that can be connected to the SUBJECT(s) responsible for this offense for the evidence sought in this affidavit.

Affiant further requests permission to search the person of the SUBJECT(s) and all other persons found at and associated with the PREMISES, such as co-occupants, for the evidence sought in this affidavit.

19) Overcoming Locked Containers & Security Measures

Affiant will make every effort to gain entry into all implements of storage (safes, lock boxes, etc.) through means that would result in minimal or no damage to these containers. However, affiant requests permission to force entry

into any implements of storage when necessary and, in the case of locked containers, after the owner/custodian has been afforded the opportunity to grant access and refused.

In addition, Affiant will make every effort to gain entry into all implements of electronic storage (computers, cell phones, & electronic storage devices) through means that would result in minimal or no damage to these devices. However, affiant requests permission to use forensic methods which are destructive when reasonable alternatives to search data on the device does not exist or when it is required to bypass a security measure and the device owner has been afforded the opportunity to provide the necessary information to access the device and refused.


Affiant requests permission to compel the owner of any computer, cellular telephone, or electronic storage device to unlock the device if said device is secured through means of biometric authentication (ex. fingerprint or facial recognition), is found at the PREMISES, and is subject to search.

Affiant requests permission to search and seize the necessary information and records such as account information, passwords, keys, and encryption keys necessary to gain access into computers, computer systems, electronic storage devices, and cellular phones in order to search for the items sought in this affiant.

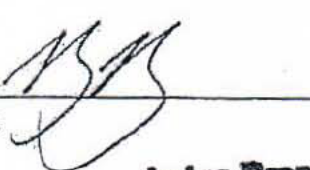
As used in this affidavit, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (visual materials).

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to me, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

WHEREFORE, Your Affiant prays for the issuance of a search warrant that will authorize him, or any peace officer of the State of Texas, to search said suspected place and premises for said property, evidence, and items and seize the same.


Affiant

Subscribed and sworn to before me by said Affiant on the 20 day February, 2018.


Printed Name

Judge Brandon Birmingham
292nd Judicial District Court
133 N. Riverfront Blvd., LB 13

Signature

DISTRICT COURT JUDGE Dallas, Texas 75207
IN AND FOR THE STATE OF TEXAS
COUNTY OF DALLAS

Attachment A – 9920 Strait Lane, Dallas, Dallas County, Texas

